

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

USDC SDNY DOCUMENT ELECTRONICALLY FILED DOC #: DATE FILED: 3/28/2025
--

CALIFORNIA FRANCHISE TAX BOARD,

Plaintiff/Counterclaim Defendant,

v.

Case No.: 1:24-cv-00683-MKV

FEDERAL DEPOSIT INSURANCE
CORPORATION, as receiver for SIGNATURE BANK,

Defendant/Counterclaim Plaintiff.

ESI PROTOCOL GOVERNING PRODUCTION OF DOCUMENTS

Pursuant to Fed. R. Civ. P. 26 and the Local Rules of this District Court, it is ORDERED that the Parties and their respective counsel shall be governed by the terms and conditions concerning the production of electronically stored information (“ESI”) and documents by the California Franchise Tax Board (“FTB”) and the Federal Deposit Insurance Corporation (“FDIC”) as Receiver for Signature Bank (the “FDIC-R”) as follows:

1. This Protocol applies to the ESI provisions of Fed. R. Civ. P. 16, 26, 33, 34, and 37, and governs the production of ESI in this Action in response to any discovery request served under the Federal Rules of Civil Procedure, and, insofar as it relates to ESI, this Protocol applies to Fed. R. Civ. P. 45 in all instances where the provisions of Fed. R. Civ. P. 45 are the same as, or substantially similar to, Fed. R. Civ. P. 16, 26, 33, 34, or 37. Nothing contained herein modifies Fed. R. Civ. P. 45 and, specifically, the provision of Rule 45(d)(2)(B) regarding the effect of a written objection to inspection or copying of any or all of the designated materials or premises. Compliance with this Protocol shall satisfy and discharge the Parties’ obligations to respond to the requests for production of documents unless otherwise agreed to by the Parties or ordered by the Court.

2. In this Protocol, the following terms have the following meanings:

a. “Metadata” means: (i) information embedded in a Native File that is not

ordinarily viewable or printable from the application that generated, edited, or modified such Native File; and (ii) information generated automatically by the operation of a computer or other information technology system when a Native File is created, modified, transmitted, deleted, or otherwise manipulated by a user of such system; and (iii) information created by the processing of a file into the format used by a reviewable database (e.g., BegBates, BegAttach). Metadata is a subset of ESI.

- b. “Native File(s)” means ESI in the electronic format of the application in which such ESI is normally created, viewed, and/or modified. Native Files are a subset of ESI.
- c. “Static Image(s)” means a representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on standard computer systems. A Static Image may be provided in Tagged Image File Format (TIFF, or .TIF files) or in Portable Document Format (PDF). If load files or OCR text files (Optical Character Recognition files) were created in the process of converting Native Files to Static Images, or if load files may be created without undue burden or cost, the Parties may provide the Load Files as set forth in Exhibit A.
- d. “Load File(s)” means the file necessary to load data into a reviewable database. A load file can, for example, specify what individual pages belong together as a document, what attachments are included with a document, where a document begins and ends, and what metadata is associated with a document.
- e. “Party” or “Parties” include the FDIC-R and the FTB and any person or entity that is served with a subpoena pursuant to Fed. R. Civ. P. 45 and opts-in to the Protocol.
- f. “Producing Party” shall mean the party that produced the data or documents at issue.

g. “Receiving Party” shall mean the party that received the data or documents at issue.

h. “Confidential Records” shall have the same meaning as defined in the Agreed Protective Order filed with this Court (the “Protective Order”) (Doc. 41).

3. The provisions set forth in Attachment “A” apply to the production of ESI for all the Parties.

4. The Parties may agree in writing (including by email) to modify, delete, or add to any of the provisions of this Protocol at any time, without the necessity of Court intervention.

5. The Parties agree that the Protective Order constitutes a Federal Rule of Evidence 502(d) order. Accordingly, none of the Parties shall be subject to the requirements outlined in Federal Rule of Evidence 502(b). Pursuant to Rule 502(d) and the Protective Order, no applicable attorney-client privilege, attorney work product, or any other applicable privilege or ground for withholding production (hereinafter, “Privilege”) is waived by production of documents or disclosure of information pursuant to this Protocol, in which event the disclosure is also not a waiver in any other federal or state proceeding. Upon demand, the Receiving Party shall return or destroy any paper copies to the Producing Party and delete or render inoperable all electronic copies of ESI that the Producing Party believes to be privileged or otherwise protected from disclosure. Confidential Records saved on back-up media in an electronically stored format will be deemed to comply with the provision if the Receiving Party has taken steps to ensure that the data destruction policy for the back-up media will result in the eventual destruction or overwriting of the requested information. In the event of a dispute regarding the claim of privilege, the receiving party may retain a copy of the material for in camera review in support of the appropriate discovery motion. Similarly, each Party has a duty to notify a Producing Party if they reasonably believe that the ESI such Party produced contains information that may be protected by the attorney-client privilege, work-product doctrine, or any other applicable privilege or ground for withholding production. To the extent that the Parties disagree over the application of these principles to any such production or challenge to the privileged nature of such material, the receiving Party shall not make use of the material in

question until the matter is resolved by the Court.

6. Nothing in this Protocol requires the Parties to produce again any information that was produced to the other prior to the execution of this Protocol.

A. FDIC-R's Bank ESI

7. The FDIC-R maintains ESI that the FDIC-R or its contractors (1) obtained from the computers, servers, and other data storage systems of Signature Bank ("the Bank") stored by the Bank prior to failure, or (2) created by scanning hard-copy records of the Bank (collectively, the "Bank ESI"). The Bank ESI is maintained by the FDIC-R in its FDIC Business Data Services ("FBDS") databases. Bank ESI is separate from the FDIC-R's post-failure receivership ESI that the FDIC-R is searching with search terms consistent with this ESI Protocol.

8. The Parties agree that the FDIC-R is not required to use search terms on the Bank ESI. Notwithstanding this limitation, the FDIC-R shall make reasonable efforts to search the Bank ESI without undue burden or cost to the FDIC-R and to the extent such efforts are necessary to identify documents responsive to the FTB's requests for production. The FDIC-R is not required to search the Bank ESI to the extent responsive documents have been identified by the FDIC-R's use of search terms on the FDIC-R's post-failure receivership ESI.

B. General

9. If a Party is in possession of certain ESI that is responsive to discovery requests propounded by the other Party, and it would not be unduly burdensome or otherwise objectionable to produce such ESI, including without limitation, e-mail and documents of various types, subject to the terms of this Protocol and the Protective Order, the Parties shall produce non-privileged ESI that is responsive to any request for production of documents. The Parties reserve the right to make physical paper documents available for inspection to the extent permitted by Federal Rule of Civil Procedure 34.

10. Each Party agrees search terms will assist in identifying documents that are responsive to the Parties' requests for production and that the application of search terms is an efficient and effective method of identifying responsive documents.

11. Each Party agrees to develop search terms and apply the search terms to the Party's ESI, subject to the terms in this Protocol and the Protective Order.

12. Upon request, each Party agrees to disclose the search terms that the Party developed and applied to identify responsive documents.

13. If a Party reasonably believes additional or modified search terms are required from the other Party to identify responsive documents without undue burden and cost, the Parties shall meet and confer in a collaborative process and in good faith to develop modified search terms.

14. During this collaborative process to establish agreed-upon modified search terms, the Parties will modify the search terms based upon the approximate volume of data and "hit" counts from the previous iteration of searching. The Parties may request a reasonable number of iterations to establish the final set of modified search terms. The Parties reserve the right to contest the proposed modified search terms and requests, including objections based upon relevancy, burdensomeness, or cost. The Parties will confer in good faith to resolve any disagreement regarding any proposed modified search terms or any other part of the search term procedure.

15. If during this collaborative process the Parties are unable to agree upon a final set of modified search terms or any other part of the search term procedure, any Party may within a reasonable time raise the issue with the Court.

16. After each Party has developed search terms or has modified search terms by the agreement of the Parties or with the assistance of the Court as provided in this Protocol, each Party shall apply the search terms to create a production set of files. Subject to the provisions in this Protocol and the Protective Order and the Bank Secrecy Act or other laws, regulations, or protections preventing the disclosure of particular information, the files will be produced in the formats permitted by Exhibit A hereto.

17. The Parties need not re-produce responsive documents that have already been produced, with the caveat that each Party reserves the right to request re-production of certain documents where circumstances may reasonably warrant, and each Party reserves the right to object to any such request.

18. Each party is responsible for taking reasonable and proportional steps to preserve potentially relevant ESI within its custody or control.

19. To the extent reasonably possible, the Parties will collect and preserve ESI in a manner that that preserves Metadata. As provided for herein, each party should reasonably endeavor to remove duplicates from all ESI productions in a consistent and defensible manner that does not break up document families (such as emails and attachments). However, the Parties should preserve any duplicate ESI that is not produced according to applicable retention and destruction policies.

20. The Parties will discuss in good faith any preservation issues that arise during the course of discovery.

21. When searching for, reviewing, and/or producing responsive ESI, each Party may apply the following reasonable cost-saving measures: clustering or concept searching, de-duplication and near de-duplication (subject to the specifications in Attachment A), e-mail thread suppression, file-type culling, and/or technology-assisted review or computer-assisted review.

22. Notwithstanding the provisions of this Protocol, each Party shall produce any and all ESI it intends to rely upon in support of any claim or defense with respect to this case.

23. If, after reviewing a Producing Party's production, the Receiving Party believes additional responsive documents exist but have not been produced, the Parties shall meet and confer in good faith and attempt to reach an agreement regarding any additional steps to be taken to locate and produce such documents and information, including but not limited to, additional means to identify documents, additional custodians to search, and the costs involved in taking such steps and any subsequent production. If the Parties are unable to reach an agreement, they may address this issue with the Court on an expedited basis.

24. Upon demand, the Receiving Party shall return or destroy any privileged or protected paper copies to the Producing Party and delete or otherwise destroy all electronic copies of privileged or protected ESI produced pursuant to this Protocol, other than any copies created as a result of a disaster recovery backup procedure.

25. The return or destruction of a document or materials over which the Producing Party has asserted a claim of Privilege as set forth above shall be without prejudice to the Receiving Party's right to contest the claim of Privilege, including seeking an order from the Court directing the production of the document on the ground that the claimed Privilege is invalid or inapplicable; provided, however, that mere production of the document or information in the course of this action shall not constitute grounds for asserting waiver of the Privilege.

26. If the Parties disagree over the application of these principles or challenge the privileged nature of produced ESI, the Receiving Party shall not make use of the ESI in question until the matter is resolved by the Court.

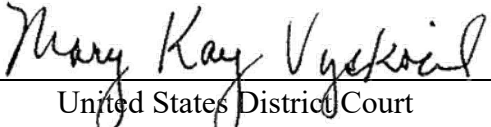
27. If a Party withholds any file on the basis of Privilege, other than communications between a Party and its counsel, it shall provide a categorical privilege log. The Parties agree that the FDIC-R is not required to provide any kind of identification of the documents withheld from production as protected by the Bank Secrecy Act.

28. All ESI and paper documents produced pursuant to this Protocol are subject to the Protective Order. Any person in possession of Confidential Records shall maintain a written information security program that includes reasonable administrative, technical, and physical safeguards to protect the security and confidentiality of such Confidential Records, protect against any reasonably anticipated threats or hazards to the security of such Confidential Records, and protect against unauthorized access to Confidential Records. To the extent a party or person does not have an information security program, they may comply with this provision by having the Confidential Records managed by and/or stored with eDiscovery vendors that maintain such an information security program. If a Receiving Party or Authorized Recipient discovers any loss of Confidential Records (including any loss of data as a result of a ransomware incident) or a breach of security, including any actual or suspected unauthorized access, relating to another Party's Confidential Records, the Receiving Party or Authorized Recipient shall: (1) promptly provide written notice to the Producing Party of such breach; (2) investigate and make reasonable efforts to remediate the effects of the breach, and provide the Producing Party with assurances reasonably

satisfactory to the Producing Party that such breach shall not recur; and (3) provide sufficient information about the breach that the Producing Party can reasonably ascertain the size and scope of the breach and/or security incident. The Receiving Party or Authorized Recipient agrees to cooperate with the Producing Party and/or law enforcement in investigating any such security incident. In any event, the Receiving Party or Authorized Recipient shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access.

29. Nothing in this Protocol shall waive or otherwise prejudice the Parties' rights to object to opposing party's requested search terms on grounds provided by the Federal Rules of Evidence, the Federal Rules of Civil Procedure, or other controlling law. As such, the Parties reserve the right to contest and object to opposing party's requested search terms based upon burdensomeness, cost, any applicable privilege, or any other applicable protection from disclosure.

SO ORDERED this 28 day of March, 2025.


United States District Court

Consented to by:

Dated: Los Angeles, California
March 26, 2025

Dated: New York, New York
March 26, 2025

GREENBERG TRAURIG, LLP

By: /s/ Rachel J. Yoo
Rachel J. Yoo
300 S. Spring St., Suite 1702
Los Angeles, CA 90013
Rachel.Yoo@doj.ca.gov

*Counsel for Plaintiff/Counterclaim
Defendant California Franchise Tax
Board*

By: /s/ Shail P. Shah
Barbara T. Kaplan
Glenn Newman
One Vanderbilt Avenue
New York, New York 10017
kaplanb@gtlaw.com
newmang@gtlaw.com
Shail P. Shah (Admitted *Pro Hac Vice*)
101 Second Street, Suite 2200
San Francisco, California 94105
Shail.Shah@gtlaw.com

*Counsel to Defendant/Counterclaim
Plaintiff Federal Deposit Insurance
Corporation, as Receiver for Signature
Bank*

Attachment A: Electronically Stored Information (ESI) and Images Specifications**1. Production Format of Native ESI**

ESI may be produced as Native Files with Load Files (DAT/OPT) that can be loaded into a document review platform such as Relativity®, Clearwell®, etc, as well as in imaged format (as discussed in section 2 below). Any produced Load Files will use the format found at subsections 2(B)-2(E).

The following categories of ESI may be produced natively:

A. Spreadsheets and Presentation Files (e.g., Excel (.xls), .csv, PowerPoint (.ppt))**B. E-mails and E-mail Repositories (e.g., Outlook .MSG/.PST, Lotus NSF, etc.)**

- i. Native e-mail may be produced to the extent that the entire e-mail family—e-mail and all attachments—is responsive, relevant and not privileged.
- ii. Upon prior agreement with the Receiving Party, a Producing Party may produce Outlook .PST and Lotus Notes .NSF e-mail files in native (*i.e.*, container) format. A separate production folder will be provided for each Custodian.

C. Structured Data: Data produced from Structured Databases may be produced in .csv or .xls format.**D. All Other ESI (e.g., Word, PDF, Apple-type files):** All other types of ESI, whether produced as Native Files or Static images, may be produced with an accompanying Load File complete with full text extracts and the fields of metadata listed in Attachment B, to the extent the metadata is available.**E. Other Potentially Relevant Sources of ESI:** The Parties will confer if they anticipate producing any potentially responsive ESI from the data sources below, and any other file formats that may require special handling, processing, or delivery methods.

- i. Instant Messenger (IM), Voicemail Data, Audio Data, Video Data, etc. (e.g., GoTo Meeting®, WebEx®);
- ii. Social Media (e.g., Twitter, Facebook, Google+, LinkedIn).

2. Production Format of Images

Responsive images produced in the format outlined below. Items to be produced in imaged format (e.g., TIFF/PDF) may include, among others, scanned hard copies and e-

mail families in which one or more items are privileged or non-responsive. In the case of e-mail, privileged or non-responsive items will be either redacted in part, or replaced by a slipsheet if withheld in its entirety.

- A. Image File Format:** Images, paper documents scanned to images, or image-rendered ESI, may be produced as 300 dpi single-page TIFF files, CCITT Group IV (2D Compression) in black and white. Images will be uniquely and sequentially Bates-numbered and unless otherwise specified, Bates numbers will be branded into each and every image.
- i. All TIFF file names shall include the unique Bates number burned into the image. All TIFF image files will be stored with the “.tif” extension.
 - ii. All scanned paper documents must be OCR’d. The resulting document-level text files may be produced with the link to the text file for a given record within the accompanying DAT Load File (see subsection 2(D) below).
 - iii. All documents will be produced in black and white TIFF format. Where the original of a produced document is in color, and color is material to the interpretation of the document, the document may be produced in color (whether in ESI or hard copy paper format). Images identified as requiring color will be produced as color 300 dpi single-page JPEG files.
 - iv. Alternatively, the Static Image can be provided in Portable Document Format (PDF). The same production format provisions apply to PDF files as applied to TIFF files in this section (i.e., subsections 2(A)(i), 2(A)(ii), 2(A)(iii), 2(B)-2(F). The Producing Party may produce PDF files with embedded text (“Searchable PDFs”).
- B. Concordance® Image Cross Reference file (i.e., .OPT):** Images may be accompanied by a Concordance® Image Cross Reference file that associates each unique identification number with its corresponding single-page TIFF image file. Any produced Cross-Reference file will also contain the image file path for each unique identification number. Image Cross Reference Sample Format:
- Unique DOCID,Volume,.\Volume\Images\IMG001\Unique DOCID.TIF,Y,,
 Unique DOCID-001,Volume,.\Volume\Images\IMG001\Unique DOCID-
 001.TIF,Y,,
 Unique DOCID-002,Volume,.\Volume\Images\IMG001\Unique DOCID-
 002.TIF,Y,,
- C. Concordance® Load File (i.e., DAT):** Images may also be accompanied by a “text load file” containing delimited text that will populate fields in a searchable, flat database environment.

- i. Text delimited load files are defined using the standard Concordance delimiters. For example:

<i>Field Separator</i>	¶ or Code 020
<i>Text Qualifier</i>	p or Code 254

- ii. This load file will also contain links to applicable native files, such as Microsoft Excel or PowerPoint files.
- iii. There will be one line for every item in a production.

D. Extracted/OCR Text: Text may be provided for each document as a separate single text file. The file name will match the unique identification number for that specific record and be accompanied by the .txt extension. A link to the text file for every record will be provided in the TEXTLINK field in the DAT file.

E. Bates Numbering Convention:

- i. All images must be assigned unique identification numbers prior to production. Each unique identification number will be uniform, include leading zeros in the number, and be unique for each produced page. Numbers will be endorsed on the actual images at a location that does not obliterate, conceal, or interfere with any information from the source document. Unless otherwise agreed upon between the Parties, the first party to enter a native-produced document as a deposition, trial, and/or other demonstrative exhibit will Bates-number the document with the unique identification number, sequentially numbers, and produce it to the other Party prior to entry as an exhibit in the underlying matter.
- ii. Native files will be assigned a single unique identification number for the entire file which will represent the native document in the Load File. The Load File will include a reference to the native file path and utilize the NATIVELINK metadata field.
- iii. Unless otherwise agreed upon between the Parties, the first party to enter a native-produced document as a deposition, trial, and/or other demonstrative exhibit will Bates-number the document with the unique identification number, sequentially numbers, and produce it to the other Party prior to entry as an exhibit in the underlying matter.

F. Document Unitization: All imaged hard copy materials will reflect accurate document unitization, including all attachments.

- i. Unitization in this context refers to identifying and marking the boundaries of documents within the collection, where a document is defined as the

smallest physical fastened unit within a bundle—*i.e.*, physical boundary (e.g., staples, paperclips, rubber bands, folders, or tabs in a binder).

3. **Directory and Folder Structure:** The directory structure for productions will be:

\CaseName\LoadFiles

\CaseName\Images < For supporting images (can include subfolders as needed, will not include more than 5,000 files per folder)

\CaseName\Natives <Native Files location (can include subfolders as needed, will not include more than 5,000 files per folder)

\CaseName\Text <Extracted Text files location (can include subfolders as needed, and up to 5,000 files per folder)

4. **Other Specifications**

A. De-Duplication: To avoid the production of more than one copy of a particular unique item, Producing Parties will use industry standard MD5 (or SHA-1) hash values within (1) all e-mails identified for production, and (2) all loose electronic files identified for production. The Producing Party will not de-duplicate attachments to e-mails against loose electronic files.

B. Media Formats for Delivery of Production Data: Electronic documents and data will be delivered via secure file sharing and transfer service (e.g., Secure FTP, ShareFile) unless the size of the data requires external media. Media will be labeled with the case caption or case name, date of the production, complete Bates range, and name of the Producing Party.

Attachment B: Metadata/Database Fields

A “✓” denotes that the indicated field should be present in the load file produced. Metadata should be included to the extent available and left empty if unavailable.

Field name	Field Description	Hard Copy	E-mail	Other ESI
NATIVEID / DOCID	Unique document Bates # or populate with the same value as Start Bates (DOCID = BEGDOC#).	✓	✓	✓
BOX #	Scanned box # record is from.	✓		
BEGBATES	Start Bates (including prefix) - No spaces.	✓	✓	✓
ENDBATES	End Bates (including prefix) - No spaces.	✓	✓	✓
GROUP IDENTIFIER	Contains the Group Identifier for the family, in order to group files with their attachments.	✓	✓	✓
BEGATTACH	Start Bates number of first attachment.	✓	✓	✓
ENDATTACH	End Bates number of last attachment.	✓	✓	✓
CUSTODIAN	Custodian/Source - format: Last, First or ABC Dept.	✓	✓	✓
AUTHOR	Creator of the document		✓	✓
FROM	Sender of an Email		✓	
TO	Recipient - format: Last name, First name.		✓	✓
CC	Carbon Copy Recipients - format: Last name, First name.		✓	✓
BCC	Blind Carbon Copy Recipients - format: Last name, First name.		✓	✓
TITLE	Document Title.		✓	✓
SUBJECT	Subject line		✓	✓
DOCDATE	Last Modified Date for files and Sent date for e-mail, this field inherits the date for attachments from their parent.		✓	✓
SENTDATE	Date Sent.		✓	
SENTTIME	Time Sent (Use GMT time zone).		✓	
CREATEDATE	Date Created.		✓	✓
CREATEDTIME	Time Created (Use GMT time zone).		✓	✓
MODDATE	Date Last Modified.		✓	✓
FILEPATH / COMPPATH	The original location of the file in the file system		✓	✓
FILENAME	File name - name of file as it appeared in its original location.		✓	✓

Field name	Field Description	Hard Copy	E-mail	Other ESI
FILE EXTENSION	.xls, .pdf, .wpd, etc.		✓	✓
DOCTYPE	Email, attachment, edoc, etc.		✓	✓
RECTYPE / APPLICATION	Application used to create native file (e.g., Excel, Outlook, Word).		✓	✓
MD5 HASH	MD5 Hash value (used for deduplication or other processing) (e-mail hash values must be run with the e-mail and all of its attachments).		✓	✓
GROUP CUSTODIAN	Name(s) of custodian(s) with exact copy of file before de-duplication		✓	✓
TEXTLINK	file path to load the text file of the extracted text or the OCR text for each record.	✓	✓	✓
NATIVELINK	file path to the load the native file for each record.		✓	✓

+ Any other fields considered relevant by the producing party.